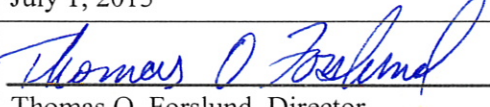
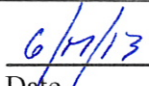


Thomas O. Forslund, Director

Governor Matthew H. Mead

Policy Title:	Report and Response to Privacy Violations and Security Incidents	
Policy Number:	AS-009 and S-006a	
Effective Date:	July 1, 2013	
Approved By:	 Thomas O. Forslund, Director	 Date

Purpose:

This policy establishes both Wyoming Department of Health's (WDH) report and response process for suspected or known security incidents and its complaint process for privacy violations.

Scope:

This policy applies to all WDH workforce.

Definitions:

Computer Incident means a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Individual means a person who is the subject of protected health information (PHI).

Security means protecting PHI (in all media) through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Security Incident means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

WDH Compliance Office means the office designated to facilitate the implementation and oversight of activities relating to the privacy and security of PHI and electronic protected health information (ePHI).

Workforce means employees, volunteers, trainees and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Policy:

Incidents or violations of WDH policies and procedures may occur despite security and confidentiality protections. Early detection and response to incidents and violations is critical to stop or correct the problem, and mitigate any harm. In appropriate cases, a thorough investigation is necessary to assess the violation or incident, mitigate any harm, determine how to prevent recurrence, and provide a basis for any disciplinary action. Therefore, all WDH workforce shall know how to report a suspected or known privacy violation or security incident.

1. General

- a. WDH workforce members shall report any:
 - i. Suspected or known privacy violations or security incidents.
 - ii. Suspected or known violation of WDH policies and procedures regarding the security or confidentiality of PHI.
 - iii. Suspected or known violation of WDH policies and procedures regarding, or the improper use of, computer and/or other information systems.
- b. Reporting and responding appropriately to suspected or known privacy violations and/or security incidents is critical to:
 - i. Minimize the frequency and severity of a violation/incident.
 - ii. Ensure early assessment and investigation before crucial evidence is diminished.
 - iii. Stop a violation/incident, correct problems, and mitigate damages.
 - iv. Ensure appropriate measures are implemented to prevent recurrence.
 - v. Ensure appropriate disciplinary actions are applied against offenders.

2. Reporting a Privacy Complaint

- a. WDH provides a process for individuals to file a complaint if they feel their privacy rights have been violated. Individuals may also file a complaint concerning WDH's failure to comply with its privacy and security policies and procedures or the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.
- b. When an individual communicates a HIPAA-related complaint to any WDH workforce member, the workforce member shall immediately notify the WDH Compliance Office.
- c. Upon receipt of a complaint, the WDH Compliance Office shall research the issue and gather any additional information necessary. If the issue can be resolved immediately, the WDH Compliance Office shall respond to the individual who filed the complaint and inform the individual of the resolution. If further research is needed, the final response and documentation may be delayed until the WDH Compliance Office is confident the issue has been thoroughly researched.
- d. All complaints shall be reported to the WDH Compliance Office as soon as possible following the filing of the complaint.
- e. WDH shall attempt to correct the violation/incident to the extent practicable within thirty (30) calendar days of the date the violation/incident was known to a WDH workforce member. WDH shall mitigate any known harmful effect of a use or disclosure of PHI in violation of WDH's policies and procedures.
- f. All complaints and resulting disposition of a complaint must be documented and retained by WDH for six (6) years.
- g. Any reports generated in response to a complaint are considered to be created in anticipation of litigation, are not discoverable, are not a client/patient care record, and shall not be made a part of the client/patient record.

3. Reporting a Security Incident

WDH will not take any adverse action against a person who reports a suspected or known incident or a violation of WDH policies and procedures. All WDH workforce should not only feel free to report a security incident without fear of retaliation, but should also understand they have a duty to do so. The WDH Compliance Office should be alerted of any incident in accordance with the provisions of section a. and b., as listed below.

- a. Security incident process.
 - i. Divisions/programs/facilities shall ensure that reporting an incident is a simple process.
 - ii. The person discovering the suspected or known incident shall initiate the reporting process as soon as possible. The person discovering the incident shall take the following actions:
 - A. Report the incident to the WDH Compliance Office using Forms SF-002, Incident Reporting Form, and SF-003, Incident Communication Log.

- B. Initiate any immediate corrective action(s), as necessary. For example, if a data user detects an unauthorized person observing PHI on a computer screen, the data user should cover the screen, turn off the screen, or otherwise prevent the unauthorized person from continuing to view it.
- C. As soon as possible, submit a written report to the WDH Compliance Office which contains the following information:
 - I. Name of person submitting the report;
 - II. Date and time of the report;
 - III. Date and time of the incident;
 - IV. Location of the incident;
 - V. Type of health information resources involved (e.g., hardware, software, data);
 - VI. Name of persons involved (i.e., suspect, witnesses);
 - VII. Nature of the security incident;
 - VIII. Harm observed, if any;
 - IX. Any statements made by suspects and witnesses;
 - X. Who was notified;
 - XI. Remedial action(s) taken, if any; and
 - XII. Any recommendations for corrective action.
- b. Computer security incident process.
 - i. Report the incident to the WDH Compliance Office using Forms SF-004, Computer Incident Reporting Form, and SF-006, Incident Contact List.
 - ii. Report the incident to the ETS Security Officer using Forms SF-004, Computer Incident Reporting Form, and SF-006, Incident Contact List.
 - iii. Record all findings using the SF-004, Computer Incident Reporting Form.
 - iv. Record all communications using Form SF-003, Incident Communication Log.
- c. All forms referenced in sections a. and b. above are located on the WDH Intranet. Once completion of a form is initiated, the form becomes an official investigative document and is, therefore, both confidential and not subject to inspection and copying by members of the public.

Contacts:

De Anna Greene, CIPP/US, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer, (307) 777-8664
Tate Nuckols, JD, WDH Security Officer, (307) 777-2438

Forms:

SF-002; Incident Reporting Form
SF-003; Incident Communication Log
SF-004; Computer Incident Reporting Form
SF-006; Incident Contact List

References:

45 CFR § 160.103
45 CFR § 164.304
45 CFR §§ 164.308(a)(2) and (6)
45 CFR § 164.316(b)(2)(i)
45 CFR §§ 164.530(a)(1)(i) and (ii)
45 CFR §§ 164.530(d)(1) and (2)
45 CFR § 164.530(g)
45 CFR § 164.530 (j)(2)
NIST SP-800-61

Training: